PTO/SB/08A (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	10/078,252
Filing Date	February 16, 2002
First Named Inventor	North, Greg
Art Unit	2818
Examiner Name	
Attorney Docket Number	501143.000024

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	US-6,341,299	01-22-2002	Romain	
	A2	US-6,157,955	12-05-2000	Narad et al	
	A3	US-6,151,393	11-21-2000	Jeong	
	A4	US-6,141,705	10-31-2000	Anand et al	
	A5	US-6,134,244	10-17-2000	Van Renesse et al	
	A6	US-6,088,453	07-11-2000	Shimbo	
	A7	US-5,987,574	11-16-1999	Paluch	
	A8	US-5,983,299	11-09-1999	Qureshi	
	A9	US-5,764,554	06-09-1998	Monier	
	A10	US-5,724.279	03--03-1998	Benaloh et al	
	A11	US-5,699,537	12-16-1997	Sharangpani et al	
	A12	US-5,542,061	07-30-1996	Omata	
	A13	US-4,799,149	01-17-1989	Wolf	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number[4]- Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	12/08/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 3

Complete if Known	
Application Number	10/078,252
Filing Date	February 16, 2002
First Named Inventor	North, Greg
Group Art Unit	2818
Examiner Name	
Attorney Docket Number	501143.000024

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	~~C1~~	~~MENEZES, A.J., et al "Efficient Implementation" from theHandbook of Applied Cryptography, (Boca Raton, CRS Press, 1997), pp. 591-607.~~ (No Copy)	
CM	C2	DIMITROV, V. and COOKLEV, T., "Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics" IEICE Trans. Fundamentals, Vol. E78-A, No. 1, January 1995.	
CM	C3	KOC, C.K. and HUNG, C.Y., "Carry-Save Adders for Computing the Product AB Modulo N" Electronics Letters, Vol. 26, No. 13, (June 21, 1990), pp. 899-900	
CM	C4	FREKING, W. L. and PARHI, K.K., " Montgomery Modular Multiplication and Exponentiation in the Residue Number System" Proc. 33rd Asilomar Conf. Signals Systems and Computer, October 1999, pp. 1312-1316.	
CM	C5	TENCA, A.F. and KOC, C.K., "A Scalable Architecture for Montgomery Multiplication" in: KOC, C.K. and PAAR, C., Cryptographic Hardware and Embedded Systems, CHES 99, Lecture Notes in Computer Science, No. 1717. 1998, New York, NY: Springer-Verlog, 1999.	
CM	C6	KOC, C.K. and ACAR, T., " Montgomery Multiplication in GF (2k)" 3rd Annual Workshop on Selected Areas in Cryptography, (August 15-16, 1996), pp. 95-106.	
CM	C7	BAJARD, J.C., et al "An RNS Montgomery Modular Multiplication Algorithm" IEEE Transactions on Computer, Vol. 47, No. 7, (July 1998), pp. 766-776.	
CM	C8	ELDRIDGE, S.E., "A Faster Modular Multiplication Algorithm" International Journal of Computer Math, Vol. 40, (1991), pp. 63-68.	
CM	C9	BOSSALAERS, A.., et al "Comparison of Three Modular Reduction Functions" In Douglas R. Stinson, editor, Advances in Cryptology - - CRYPTO '93, Vol. 773 of Lecture Notes in Computer Science, (August 22-26, 1993), pp. 166-174.	
CM	C 10	MONTGOMERY, P.L., "Modular Multiplication Without Trial Division" Mathematics of Computation, Vol. 44, No. 170 (April 1985), pp. 519-521.	
CM	C 11	KOC, C.K., et al "Analyzing and Comparing Montgomery Multiplication Algorithms" IEEE Micro, Vol. 16, Issue 3, (June 1996), pp. 26-33.	

Examiner Signature		Date Considered	12/08/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 3 of 3

Complete if Known	
Application Number	10/078,252
Filing Date	February 16, 2002
First Named Inventor	North, Greg
Group Art Unit	2818
Examiner Name	
Attorney Docket Number	501143.000024

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
Cu	C 12	KORNERUP, P., " High-Radix Modular Multiplication for Cryptosystems" Department of Mathematics and Computer Science, (1993), pp. 277-283.	
Cu	C 13	SUNAR, B. and KOC, C.K., "An Efficient Optimal Normal Basis Type II Multiplier" Brief Contributions, IEEE Transactions on Computers, Vol. 50, No. 1, (January 2001), pp. 83-87.	
Cu	C 14	KOC, C.K., "Comments on' Residue Arithmetic VLSI Array Architecture for Manipulator Pseudo-Inverse Jacobian Computation' " Communications, IEEE Transactions on Robotics and Automation, Vol. 7, No. 5, (October 1991), pp. 715-716.	
Cu	C 15	SAVAS, E. and KOC, C.K., "The Montgomery Modular Inverse-Revisited" IEEE Transactions on Computers, Vol. 49, No. 7, (July 2000), pp. 763-766.	
Cu	C 16	WALTER, C.D., " Montgomery's Multiplication Technique: How to Make it Smaller and Faster" in Cryptographic Hardware and Embedded Systems - CHAS 1999, C. Paar (Eds.). K. Ko, Ed. 1999, Springer, Berlin Germany, pp.61-72.	
	~~C 17~~	~~OH, H. and MOON, J., "Modular Multiplication Method" IEE Proc.-Comput. Digit.Tech., Vol. 145, No. 4, (July 1998), pp. 317-318~~ (No Copy)	
Cu	C 18	BLUM, T., " Modular Exponentiation on Reconfigurable Hardware" Master's thesis, ECE Department, Worcester Polytechnic Institute, Submitted to Faculty 1999-04-08, Published May 1999. Retrieved from the Internet <URL: http://www.wpl.edu/pubs/ETD/Available/etd-090399-090413/unrestricted/blum.pdf>. ~~No Copy~~	
Cu	C 19	MARWEDEL, P., et al. "Built in Chaining: Introducing Complex Components into Architectural Synthesis." April 1996. Proceedings of the ASP-DAC, 1997. [online]. Retrieved from the Internet <URL: http://eldorado.uni-dortmund.de:8080/FB4/ls12/forshung/1997/aspdac/aspacPDF>.	
Cu	C 20	TIOUNTCHIK, A., and TRICHINA, E., "RSA Acceleration with Field Programmable Gate Arrays" Lecture Notes in Computer Science, Vol. 1587, pp.164-176. Retrieved from the Internet: <URL:http://citeseer.nj.nec.com/274658.html>.	

Examiner Signature	NGO	Date Considered	12/08/05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/078,252
Filing Date	February 16, 2002
First Named Inventor	Greg North
Group Art Unit	2818
Examiner Name	to be assigned
Attorney Docket Number	501143.000024

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
Ck	C 21	MENEZES, A.J., et al "Handbook of Applied Cryptography" Boca Raton, CRC Press, 1997. pp. 591-607.	

Examiner Signature	NGO	Date Considered	12/8/05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.